PATENT ABSTRACTS OF JAPAN

(11)Publication number:

11-039158

(43) Date of publication of application: 12.02.1999

(51)Int.CI.

G06F 9/06 G06F 12/14

(21)Application number: 09-210006

(71)Applicant: NIPPON TELEGR & TELEPH CORP (NTT)

N T T ELECTRON KK

(22)Date of filing:

18.07.1997

(72)Inventor:

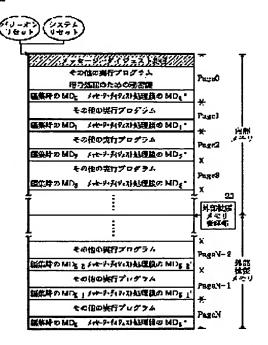
KAWAKUBO HIDEJI TAKADA SHUNSUKE YAMANAKA KIYOSHI MATSUMOTO HIROYUKI

(54) METHOD FOR PROTECTING EXECUTED PROGRAM AND ITS DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To stop reading of secret information of a processor itself by immediately stopping execution of an execution program when the execution program is detected to be forged before the specified execution program is run.

SOLUTION: A message digest processing is executed by branching a system into reset entry addresses of incorporated RUM/PROM after the system is reset. In this case, a message digest MD' is assigned to data byte obtained at the end of each processing. A message digest MD at editing is collated with the message digest MD' before which the message digest processing is executed whenever the execution program is run. And when the message digest MD at the editing and the message digest MD' after the message digest processing are not coincide, the execution program is judged to be forged and the execution of the execution program after that is stopped.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平11-39158

(43)公開日 平成11年(1999)2月12日

(51) Int.Cl. ⁶	識別記号	ΡI	
G06F 9/06	5 5 0	G06F 9/06	5 5 0 Z
12/14	3 1 0	12/14	3 1 0 Z

審査請求 未請求 請求項の数8 FD (全 8 頁)

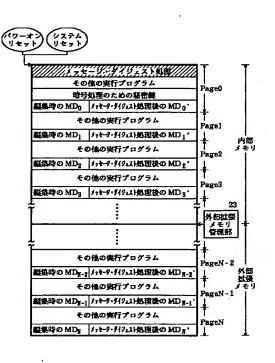
(21)出願番号	特顏平9-210006	(71) 出顧人 000004226
	•:	日本電信電話株式会社
(22)出顧日 平)	平成9年(1997)7月18日	東京都新宿区西新宿三丁目19番2号
		(71) 出顧人 591230295
		エヌティティエレクトロニクス株式会社
		東京都渋谷区桜丘町20番1号
		(72)発明者 河久保 秀二
		東京都新宿区西新宿三丁目19番2号 日本
		電信電話株式会社内
		(72)発明者 高田 俊介
		東京都新宿区西新宿三丁目19番2号 日本
		電信電話株式会社内
		(74)代理人 弁理士 川久保 新一
		最終頁に続く

(54) 【発明の名称】 実行プログラムの保護方法およびその装置

(57) 【要約】

【課題】 1チップの中にFROM(フラッシュメモリ)等のROMとRAMと処理部とが複合して構成されているLSIにおいて、処理装置自身の秘密情報(秘密鍵)の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる実行プログラムの保護方法およびその装置を提供することを目的とするものである。

【解決手段】 パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出し、この改竄検出において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止するものである。



【特許請求の範囲】

【請求項1】 パワーオンリセット後またはシステムリ セット後であって、所定の実行プログラムが走行する前 に、上記実行プログラムが改竄されていることを検出す る改竄検出段階と;上記改竄検出段階において上記改竄 が検出されると、上記実行プログラムの実行を直ちに停 止する実行停止段階と;を有することを特徴とする実行 プログラムの保護方法。

【請求項2】 請求項1において、

上記所定の実行プログラムを編集し、この編集された実 行プログラムのメッセージ・ダイジェストである編集時 のメッセージ・ダイジェストを所定のメモリに書き込む 編集時のメッセージ・ダイジェスト書き込み段階を有 し、

上記改竄検出段階は、

上記実行プログラムを暗号処理する暗号処理段階と;上 記暗号処理された実行プログラムの中から、メッセージ ・ダイジェスト処理されたメッセージ・ダイジェストで ある第2のメッセージ・ダイジェストを抽出する第2の メッセージ・ダイジェスト抽出段階と;上記第2のメッ セージ・ダイジェストと、上記編集時のメッセージ・ダ イジェストとを照合するメッセージ・ダイジェスト照合 段階と;上記メッセージ・ダイジェスト照合段階におい て照合が得られなかったときに、上記実行プログラムが 改竄されていると判断する改竄判定段階と;によって構 成されていることを特徴とする実行プログラムの保護方 法。

【請求項3】 請求項2において、

上記編集時のメッセージ・ダイジェストは、上記暗号処 理を実行しても変化しない態様で書き込まれていること を特徴とする実行プログラムの保護方法。

【請求項4】 パワーオンリセット後またはシステムリ セット後であって、所定の実行プログラムが走行する前 に、上記実行プログラムが改竄されていることを検出す る改竄検出手段と;上記改竄検出手段において上記改竄 が検出されると、上記実行プログラムの実行を直ちに停 止する実行停止手段と;を有することを特徴とする実行 プログラムの保護装置。

【請求項5】 請求項4において、

上記所定の実行プログラムを編集し、この編集された実 行プログラムのメッセージ・ダイジェストである編集時 のメッセージ・ダイジェストを所定のメモリに書き込む 編集時のメッセージ・ダイジェスト書き込み手段を有

上記改竄検出手段は、

上記実行プログラムを暗号処理する暗号処理手段と;上 記暗号処理された実行プログラムの中から、メッセージ ・ダイジェスト処理されたメッセージ・ダイジェストで ある第2のメッセージ・ダイジェストを抽出する第2の メッセージ・ダイジェスト抽出手段と;上記第2のメッ 50 バスによって接続される構成が採用されている。

セージ・ダイジェストと、上記編集時のメッセージ・ダ イジェストとを照合するメッセージ・ダイジェスト照合 手段と;上記メッセージ・ダイジェスト照合手段におい て照合が得られなかったときに、上記実行プログラムが 改竄されていると判断する改竄判定手段と;によって構 成されていることを特徴とする実行プログラムの保護装 置。

【請求項6】 請求項5において、

上記編集時のメッセージ・ダイジェストは、上記暗号処 10 理を実行しても変化しない態様で書き込まれていること を特徴とする実行プログラムの保護装置。

【請求項7】 パワーオンリセット後またはシステムリ セット後であって、所定の実行プログラムが走行する前 に、上記実行プログラムが改竄されていることを検出す る改竄検出手段と;上記改竄検出手段において上記改竄 が検出されると、上記実行プログラムの実行を直ちに停 止する実行停止手段と;としてコンピュータを機能させ るためのプログラムを記録したコンピュータ読取可能な 記録媒体。

【請求項8】所定の実行プログラムを編集し、この編集 された実行プログラムのメッセージ・ダイジェストであ る編集時のメッセージ・ダイジェストを所定のメモリに 書き込む編集時のメッセージ・ダイジェスト書き込み手 段と;上記実行プログラムを暗号処理する暗号処理手段 と;上記暗号処理された実行プログラムの中から、メッ セージ・ダイジェスト処理されたメッセージ・ダイジェ ストである第2のメッセージ・ダイジェストを抽出する 第2のメッセージ・ダイジェスト抽出手段と;上記第2 のメッセージ・ダイジェストと、上記編集時のメッセー 30 ジ・ダイジェストとを照合するメッセージ・ダイジェス ト照合手段と;上記メッセージ・ダイジェスト照合手段 において照合が得られなかったときに、上記実行プログ ラムが改竄されていると判断する改竄判定手段と;上記 改竄判断手段において上記改竄が判断されると、上記実 行プログラムの実行を直ちに停止する実行停止手段と; としてコンピュータを機能させるためのプログラムを記 録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【発明の属する技術分野】本発明は、実行プログラムを 保護する方法およびその装置に関する。

【従来の技術】従来、パーソナルコンピュータや、パー ソナルコンピュータの拡張バスに画像処理・音声処理等 の専用制御ボード等が接続され、上記専用制御ボード等 において、これらの処理や制御を実行するCPUと、プ ログラムの実行メモリ(RAM)と、実行プログラムの 保管や処理開始時や実行中に読み出し/書き込みされる データメモリ(ROM)とが、互いに別々に構成され、

3

【0003】上記構成においては、上記実行メモリ、上記データメモリの内容を、実行プログラムの実行前に、部分的に変更することが可能である。したがって、実行メモリ、データメモリの内容を、実行プログラムの実行前に、第三者が部分的に変更すれば、上記実行プログラムの実行する処理装置自身の秘密情報(秘密鍵)を読み出すことが可能であり、また、上記処理装置における意図しない動作を、第三者が外部から強制的に実行させることが可能である。

[0004]

【発明が解決しようとする課題】図5は、従来の画像処理・音声処理等の専用制御ボードCB1を示すプロック図である。

【0005】画像処理・音声処理等の専用制御ボードCB1は、処理部(CPU)11と、データメモリとしてのROM12と、実行メモリとしてのRAM13とを1チップに封入したものである。なお、符号14は、インタフェース部であり、符号15は、カード1/F部である

【0006】このように、実行メモリとデータメモリと 処理部とを 1 チップ化することによって、上記処理装置 自身の秘密情報(秘密鍵)が伝送される信号線は、上記 チップの外部に露出しないので、第三者が、チップの外部において、信号線に端子等を接触させ、上記秘密情報 (秘密鍵) を取り出す操作を実行することは不可能である。

【0007】つまり、上記の場合、信号線に端子等を接触させ、上記秘密情報 (秘密鍵)を取り出す操作を実行するためには、チップのケースを開く必要があり、そのケースを開いたとしても、チップ内部の配線のうちでどの配線に端子等を接触させればよいかの判断が極めて困難であり、また、端子等を接触させるべき配線が分かったとしても、チップ内部の微細な配線に端子等を接触させることが実際上不可能である。したがって、上記処理装置自身の秘密情報 (秘密鍵)の読み出しを阻止することができ、また、外部からの悪意による処理装置の意図しない動作を阻止することができる。

【0008】しかし、上記のように1チップ化したとしても、RAM13の内容をコピーすれば、上記処理装置自身の秘密情報の読み出しを阻止することができないという問題がある。

【0009】また、上記のように1チップ化したとしても、製造工程で用いるROM書き込み装置を利用して、ROM12の内容を改竄した場合や、RAM13を部分修正した場合には、外部からの悪意による処理装置の意図しない動作を阻止することができないという問題がある。

【0010】本発明は、1チップの中にFROM(フラ・ダイジェスト抽出手段と、上記第2のメッセージ・ダッシュメモリ)等のROMとRAMと処理部とが複合し イジェストと、上記編集時のメッセージ・ダイジェストで構成されているLSIにおいて、処理装置自身の秘密 50 とを照合するメッセージ・ダイジェスト照合手段と、上

:

情報(秘密鍵)の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる実行プログラムの保護方法およびその装置を 提供することを目的とするものである。

[0011]

【課題を解決するための手段】本発明は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出し、この改竄検出において上記 10 改竄が検出されると、上記実行プログラムの実行を直ちに停止するものである。

[0012]

【発明の実施の形態および実施例】図1は、本発明の一 実施例である実行プログラムの保護装置PP1を示すブロック図である。

【0013】実行プログラムの保護装置PP1は、CPU等で構成されている処理部21と、データメモリとしてのROM22と、実行メモリとしてのRAM23と、インタフェース部14と、カードI/F部15と、拡張ROM24と、拡張RAM25と、外部拡張メモリ管理部26とを有するものである。

【0014】また、実行メモリとしてのRAM23と、データメモリとしてのROM22と、処理部21と、インタフェース部14と、外部拡張メモリ管理部26とは、図1において太線で囲まれており、この太線内の素子が1チップ化されている。

【0015】処理部21は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段の例であり、上記改竄検出段階において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段の例である。また、処理部21は、上記所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段の例である。

【0016】なお、「メッセージ・ダイジェスト」は、 メッセージ・ダイジェストの対象となる原文(上記実施 の例においては、実行プログラム)が1ピットでも書き換 えられると、その原文についてメッセージ・ダイジェス ト処理を実行した後に、変化するものである。

【0017】さらに、上記改竄検出手段は、上記実行プログラムを暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第2のメッセージ・ダイジェスト抽出手段と、上記第2のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と、上

5

記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段とによって構成され、これらの各手段も、処理部 2 1 が実現する。なお、上記編集時のメッセージ・ダイジェストは、上記暗号処理を実行しても変化しない態様で書き込まれている。

【0018】ここで、「メッセージ・ダイジェスト」は、上記実施例においては、一方向性ハッシュ関数によって実行プログラムを処理した後における最後の16バイトのデータであり、「メッセージ・ダイジェスト処理」は、一方向性ハッシュ関数によって実行プログラムを処理する動作である。上記一方向性ハッシュ関数のアルゴリズムとしては、MD2、MD5、SHA-1等があり、これらのうちのどのアルゴリズムを使用してもよい(MD2、MD5、SHA-1については、「『暗号理論入門』 岡本栄司著 共立出版株式会社」を参照)。また、上記一方向性ハッシュ関数以外の関数を使用して実行プログラムを処理することによって、メッセージ・ダイジェストを実現するようにしてもよい。

【0019】図2は、上記実施例におけるメモリマップを示す図である。

【0020】図2に示すメモリマップは、RAM23の内部メモリの領域と、拡張RAM25の外部拡張メモリの領域とが使用され、Page0~PageNで構成されている。

【0021】Page 0には、メッセージ・ダイジェスト処理のプログラムと、その他の実行プログラムと、暗号処理のための秘密鍵と、Page 0に関する編集時のメッセージ・ダイジェストMD $_0$ と、Page 0に関するメッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD $_0$)とが格納されている。

【0022】なお、メッセージ・ダイジェスト処理する場合、上記のように、MD2、MD5、SHA-1等のうちのどのアルゴリズムを使用してもよいが、所定Pageについて編集時のメッセージ・ダイジェストを生成する場合に使用するアルゴリズムと、所定Pageについて実行プログラムを走行させる前にそのPageおいてメッセージ・ダイジェスト処理する場合に使用するアルゴリズムとが同一である必要がある。

【0023】 Page 1 には、その他の実行プログラムと、 Page 1 に関する編集時のメッセージ・ダイジェストMD 1 とが格納されている。また、メッセージ・ダイジェスト処理後には、 Page 1 に関するメッセージ・ダイジェストMD 1 が、 Page 1 に格納される。

【0024】Page 2以降の各Pageには、Page 1 における 内容と同様の内容が格納され、その他の実行プログラム と、そのPageに関する編集時のメッセージ・ダイジェス トとが格納され、また、メッセージ・ダイジェスト処理 後には、そのPageに関するメッセージ・ダイジェスト処 50 6 理後のメッセージ・ダイジェストが、そのPageに格納される。

【0025】なお、メッセージ・ダイジェスト処理は、アルゴリズムを明示しないメッセージ・ダイジェスト処理であり、各Pageのメッセージ・ダイジェストを作成する機能を有し、PageOのメッセージ・ダイジェスト処理は、各Pageのメッセージ・ダイジェストをとる。つまり、図2には、PageOにのみメッセージ・ダイジェスト処理が記載されているが、Page1以降の各Pageにおいて10メッセージ・ダイジェスト処理が実行される。

【0026】また、「実行プログラム」は、たとえば電文を外部から読み込む処理や、その読み込んだ電文に暗号処理を施す処理を記述したプログラムである。さらに、「その他の実行プログラム」は、メッセージ・ダイジェスト処理のプログラム以外の実行プログラムである。

【0027】次に、上記実施例の動作について説明する。

【0028】図3は、上記実施例において、実行プログ ク ラムの保護装置PP1を製造するときにおける動作を示 すフローチャートである。

【0029】まず、Pageの関数nを「0」とし(S1)、Page n に書き込むべき実行プログラムをロードする(S2)。そして、編集時のメッセージ・ダイジェスト MD_n を生成し(S3)、上記編集時のメッセージ・ダイジェスト MD_n を、該当Pageの最後の16バイトに書き込む(S4)。

【0030】次に、Pagenに書き込むべき実行プログラムについてメッセージ・ダイジェスト処理を実行するこ30 とによってメッセージ・ダイジェストMDn 'を生成し(S5)、1Page分のプログラムをメモリ23に書き込み、その書き込まれた内容を編集する(S6)。そして、編集された内容をPage単位でPROM22に書き込み(S7)、次のPageについて上記処理(S2~S7)を実行し(S8、S9)、最大のPageNまで上記処理(S2~S7)が終了すると、実行プログラムの保護装置PP1を製造する場合における全ての処理を終了する。

【0031】次に、上記実施例における実行プログラム 40 の保護動作について説明する。

【0032】図4は、上記実施例における実行プログラムの保護動作を示すフローチャートである。

【0033】まず、電源投入時にパワーオンリセットする(S11)か、または、システムリセットした(S12)後に、内蔵のROM/PROM22のリセット・エントリ・アドレスに分岐し、メッセージ・ダイジェスト処理を実行する(S21)。なお、各処理の最後に得られるデータ16パイトに、上記メッセージ・ダイジェストMD'を割り当てる。

50 【0034】編集時のメッセージ・ダイジェストMD

と、実行プログラムを走行する毎に、その直前にメッセージ・ダイジェスト処理が行われたメッセージ・ダイジェストMD'とを、照合手段(図示せず)が照合する(S22、S24~S31)。そして、この照合の結果、上記予め作成されている編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェストMD'とが、全てのPageにおいて一致した場合にのみ、上記実行プログラムの動作を通常通りに開始させる。

【0035】すなわち、実行プログラムに変化が加えられていなければ(改竄されていなければ)、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'が変化しないので、このメッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'は、編集時のメッセージ・ダイジェストMDと同じである。

【0036】一方、上記照合の結果、編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが一致しなかった場合(S22、S24、S32)、実行プログラムが変化されている場合であり、多くの場合、その実行プログラムが改竄されているので、その段階で、実行プログラムの実行を停止する。編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが一致しなかった場合、その実行プログラムが改竄されたと判断し、その後の実行プログラムの実行を停止する。

【0037】このようにすることによって、1チップの中にFROM(フラッシュメモリ)等のROMとRAMと処理部とが複合して構成されているLSIにおいて、実行プログラムが改竄されたと判断されると、その後の実行プログラムの実行を停止するので、処理装置自身の秘密情報(秘密鍵)の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる。

【0038】実行プログラムが大規模であれば、上記実施例のように外部拡張メモリを使い、この場合、命令によって、メモリ拡張モード・レジスタを設定する。このようにすることによって、外部メモリ領域に外部デバイスを接続できる外部拡張モードになる。

【0039】上記実施例において、実行プログラムが大規模でなければ、拡張ROM24、拡張RAM25、外部拡張メモリ管理部26を省略するようにしてもよい。 【0040】上記実施例を、装置の発明として把握すると、上記実施例は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と、上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段とを有する実行プログラムの保護装置である。 8

【0041】この場合、所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段を有し、上記改竄検出手段は、上記暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェストのメッセージ・ダイジェストを抽出する第2のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストと、上記にメッセージ・ダイジェスト照合手段において照合するメッセージ・ダイジェスト照合手段において照合れなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段とによって構成されている。

【0042】また、上記実施例を、記録媒体の発明として把握すると、上記実施例は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と、上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段ととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体である。

【0043】この場合、所定の実行プログラムを編集 し、この編集された実行プログラムのメッセージ・ダイ ジェストである編集時のメッセージ・ダイジェストを所 定のメモリに書き込む編集時のメッセージ・ダイジェス ト書き込み手段と、上記実行プログラムを暗号処理する 暗号処理手段と、上記暗号処理された実行プログラムの 中から、メッセージ・ダイジェスト処理されたメッセー ジ・ダイジェストである第2のメッセージ・ダイジェス トを抽出する第2のメッセージ・ダイジェスト抽出手段 と、上記第2のメッセージ・ダイジェストと、上記編集 時のメッセージ・ダイジェストとを照合するメッセージ ・ダイジェスト照合手段と、上記メッセージ・ダイジェ ・スト照合手段において照合が得られなかったときに、上 記実行プログラムが改竄されていると判断する改竄判定 40 手段と、上記改竄判断手段において上記改竄が判断され ると、上記実行プログラムの実行を直ちに停止する実行 停止手段ととしてコンピュータを機能させるためのプロ グラムを記録したコンピュータ読取可能な記録媒体であ る。

[0044]

【発明の効果】本発明によれば、1チップの中にFROMとRAMと処理部とが複合して構成されているLSIにおいて、処理装置自身の秘密情報の読み出しや、悪意による処理装置の意図しない動作を排除することができ 50 るという効果を奏する。

9

【図面の簡単な説明】

【図1】本発明の一実施例である実行プログラムの保護 装置PP1を示すプロック図である。

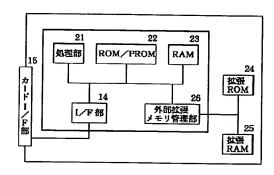
【図2】上記実施例におけるメモリマップを示す図である。

【図3】上記実施例において、実行プログラムの保護装置PP1を製造するときにおける動作を示すフローチャートである。

【図4】上記実施例における実行プログラムの保護動作のフローチャートである。

【図1】

PP1: 実行プログラムの保護装置



【図5】従来における画像処理・音声処理等の専用制御ボードCB1を示すブロック図である。

【符号の説明】

PP1…実行プログラムの保護装置、

21…処理部、

 $2 2 \cdots ROM/PROM$

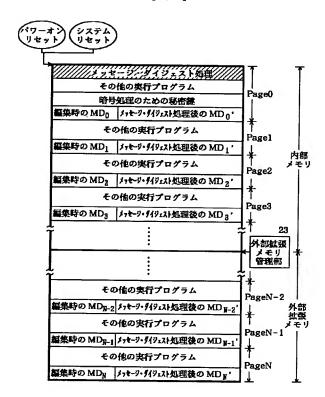
23 ··· RAM,

24…拡張ROM、

25…拡張RAM、

10 26…外部拡張メモリ管理部。

【図2】

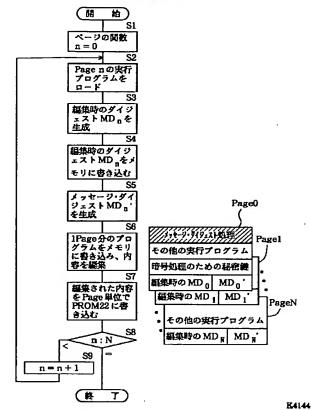


K4144

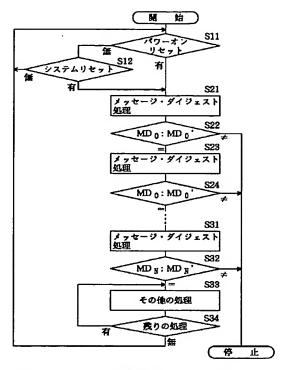
K4144

【図3】

製造時の処理手順



【図4】



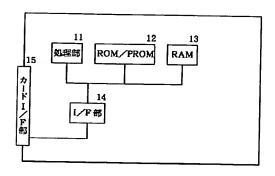
MD_n : Page n についての**個**集時のメッセージ・ダイジェスト (ROM/RAM22 に実行プログラムから書き込まれた ときのメッセージ・ダイジェスト)

MD_n': Page nに関するメッセージ・ダイジェスト処理後の メッセージ・ダイジェスト

K4144

【図5】

CB1: 従来の専用制御ボード



K4144

フロントページの続き

(72)発明者 山中 喜義

東京都新宿区西新宿三丁目19番 2 号 日本電信電話株式会社内

(72)発明者 松本 博幸

東京都渋谷区桜丘町20番1号 エヌティティエレクトロニクス株式会社内